UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,942	01/19/2001	Robert M. Fries	14531.68	7598

47973 7590 03/16/2005

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/765,942	FRIES ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-18 and 20-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-18 and 20-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-18, and 20-32 are pending in this office action. Claim 19 is canceled.

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1, 3, 9, 17, 18, and 20-22 are rejected under 35 U.S.C. 102(a) as being anticipated by Angelo et al. (U.S. Patent No. 6,625,730).

Regarding claim 1, Angelo et al. teaches in a computer system with a processing device coupled to a memory device through a bus (fig. 3. ref. num 200, 202, 204) **and a boot signature checker that is separate from the processing device** (fig. 3, ref. num 208), the computer system configured to be capable of receiving presentable content, a method of detecting tampering of the computer system, the method comprising the following:

- A specific act of booting up the computer system (fig. 4A, ref. num 306);

- A specific act of **the boot signature checker** monitoring a signal sequence that occurs on the computer system bus **coupling the processing device and memory device** during the specific act of booting up the computer system (fig. 4A, ref. num 308 and col. 1, lines 32-42 and col. 6, lines 20-30);
- A specific act of **the boot signature checker** calculating a boot signature **from** the monitored signal sequence (fig. 4A, ref. num 308);
- A specific act of comparing the calculated boot signature to an expected boot signature that represents no tampering to the computer system (fig. 4A, ref. num 312); and
- A specific act of determining that tampering has not occurred if the calculated boot signature is the same as the expected boot signature (fig. 4A, ref. num 320/322).

Regarding claim 3, Angelo et al. teaches further comprising the following: a specific act of enabling presentable content to be presented if it is determined that tampering has not occurred (col. 7, lines 40-47, the system takes actions, as opposed to disabling actions).

Regarding claim 9, Angelo et al. teaches further comprising a specific act of determining that tampering has occurred if the calculated boot signature is different than the expected boot signature (fig. 4A, ref. num 314/316).

Regarding claim 17, Angelo et al. teaches wherein the specific act of calculating a boot signature that is a function of the signal sequence comprises the following: calculating the boot signature by applying a polynomial expression to the signal sequence (col. 7, lines 7-18, the secure hash is a polynomial expression).

Regarding claim 18, Angelo et al. teaches in a computer system with a processing device coupled to a memory device through a bus (fig. 3. ref. num 200, 202, 204) **and a boot signature checker that is separate from the processing device** (fig. 3, ref. num 208), the computer system configured to be capable of receiving presentable, a method of detecting tampering of the computer system, the method comprising the following:

- A specific act of booting up the computer system (fig. 4A, ref. num 306);
- A step for **the boot signature checker** producing a boot signature that is a function of the signal sequence experienced on the computer system bus **between the processing device and the memory device** during the specific act of booting (fig. 4A, ref. num 308 and col. 1, lines 32-42 and col. 6, lines 20-30); and
- A step for determining whether the calculated boot signature is indicative of the computer system being tampered with (fig. 4A, ref. num 320/322 and 314/316).

Regarding claim 20, Angelo et al. teaches wherein the step for calculating a boot signature comprises the following:

- A specific act of monitoring the signal sequence during the specific act of booting up the computer system (col. 1, lines 32-42 and col. 6, lines 20-30); and
- A specific act of calculating the boot signature as a function of the signal sequence monitored during the specific act of monitoring (col. 7, lines 7-18).

Regarding claim 21, Angelo et al. teaches the specific act of monitoring the signal sequence comprises the following: a specific act of a boot signature checker monitoring the bus to determine the signal sequence that occurs on the local bus during the specific act of booting up the computer system (col. 1, lines 32-42 and col. 6, lines 20-30).

Regarding claim 22, Angelo et al. teaches further comprising: a step for acting on the determination of whether the calculated boot signature is indicative of the computer system being tampered with (fig. 4A, ref. num 320/322 or 314/316/318).

Claim Rejections - 35 USC § 103

5. Claims 4-8, 10-16, 23-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (USPN '730) in view of Raboswky (U.S. Patent No. 6,141,530).

Regarding claim 4, Angelo et al. teaches all the limitations of claims 1 and 3, above. However, Angelo et al. does not teach wherein the presentable content is encrypted presentable content, wherein the specific act of enabling presentable content

to be presented comprises the following: activating a decrypter that receives the encrypted presentable content.

Rabowsky teaches wherein the presentable content is encrypted presentable content, wherein the specific act of enabling presentable content to be presented comprises the following: activating a decrypter that receives the encrypted presentable content (col. 9, line 65 through col. 10, line 11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine activating a decrypter that receives the encrypted presentable content, as taught by Rabowsky, with the method of Angelo et al. It would have been obvious for such modifications because activating the decrypted when only a valid signature was found prevent the playing of data on a tampered system.

Regarding claim 5, the combination of Angelo et al. in view of Rabowsky teaches wherein the specific act of monitoring a signal sequence is performed by a boot signature checker circuit that is integrated with the decrypter (see fig. 2, connection between 72 and 74 of Rabowsky).

Regarding claim 6, the combination of Angelo et al. in view of Rabowsky teaches wherein the specific act of activating a decrypter comprises the following: a specific act of providing the calculated boot signature directly to the decrypter, wherein the

decrypter is configured to accept the expected boot signature as a key string needed to activate the decrypter (see col. 9, line 65 through col. 10, line 11 of Rabowsky).

Regarding claim 7, the combination of Angelo et al. in view of Rabowsky teaches wherein the specific act of activating a decrypter comprises the following: a specific act of providing the calculated boot signature to the decrypter; and a specific act of the decrypter obtaining a key string needed to be activated if the calculated boot signature matched the expected boot signature (see col. 9, line 65 through col. 10, line 11 of Rabowsky).

Regarding claim 8, the combination of Angelo et al. in view of Rabowsky teaches wherein the specific act of the decrypter obtaining a key string comprises the following: a specific act of the decrypter obtaining the key string from the memory device (see fig. 4, ref. num 410 of Angelo et al. and fig. 2, ref. num 78 of Rabowsky).

Regarding claim 10, Angelo et al. teaches all the limitations of claims 1 and 9, above. However, Angelo et al. does not teach further comprising the following: a specific act of blocking the presentation of the presentable content if it is determined that tampering has occurred.

Rabowsky teaches further comprising the following: a specific act of blocking the presentation of the presentable content if it is determined that tampering has occurred (col. 9, line 65 through col. 10, line 11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the act of blocking presentation of content if tampering has occurred, as taught by Rabowsky, with the method of Angelo et al. It would have been obvious for such modifications because activating the decrypter when only a valid signature was found prevents the playing of data on a tampered system.

Regarding claims 11-16, the combination of Angelo et al. in view of Rabowsky teaches wherein the specific act of blocking the presentation of the presentable content comprises the following:

- A specific act of deactivating a decrypter that receives the presentable content (see col. 9, line 65 through col. 10, line 11 of Rabowsky);
- A specific act of disabling a tuner/demodulator such that the demodulator does not demodulate the presentable content (see fig. 2, ref. num 64 of Rabowsky);
- Disabling a central processing unit clock (see fig. 2, ref. num 70 of Rabowsky);
- Disabling a demultiplexor such that audio, video or other data cannot be extracted from the presentable content (see fig. 2, ref. num 8/74 of Rabowsky); and
- Disabling a network interface device used by the computer system to interface with a network (see col. 5, line 62 through col. 6, line 4 of Rabowsky).

Although Rabowsky mainly shows deactivating a decrypter (see col. 9, line 65 through col. 10, line 11), deactivating/disabling other devices within the receiving

computer provides the same end result, that is, disabling the end user from viewing presentable content if tampering of the system was detected.

Regarding claim 23, Angelo et al. teaches all the limitations of claims 18 and 22, above. However, Angelo et al. does not teach wherein the step for acting on the determination comprises the following: a specific act of activating a decrypter so as to enable the decrypter to decrypt the presentable content.

Rabowsky teaches wherein the step for acting on the determination comprises the following: a specific act of activating a decrypter so as to enable the decrypter to decrypt the presentable content (col. 9, line 65 through col. 10, line 11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine activating a decrypter so as to enable the decrypter to decrypt the presentable content, as taught by Rabowsky, with the method of Angelo et al. It would have been obvious for such modifications because activating the decrypter when only a valid signature was found prevents the playing of data on a tampered system.

Regarding claim 24, the combination of Angelo et al. in view of Rabowsky teaches wherein the specific act of activating a decrypter comprises the following: a specific act of providing the calculated boot signature directly to the decrypter, wherein

the decrypter is configured to accept an expected boot signature as a key string needed to activate the decrypter (see col. 9, line 65 through col. 10, line 11 of Rabowsky).

Regarding claim 25, Angelo et al. teaches a computer system capable of receiving presentable content, wherein the computer system comprises:

- A processing device (fig 3, ref. num 200);
- A memory device (fig. 3, ref. num 202 and 204);
- A **local** bus coupled to the processing device and the memory device (fig. 3, the connections between processor and the two memories); and
- A boot signature checker, separate from the processing device, that is coupled to the **local** bus so as to be able to read a signal sequence asserted on the local bus during booting of the computer system (fig. 3, ref. num 208 and col. 1, lines 32-42 and col. 6, lines 20-30),
    - Wherein the boot signature checker is configured to calculate a boot signature **from** the signal sequence asserted on the local bus **coupling the processing device and the memory device** (fig. 4A, ref. num 308).

Angelo et al. does not teach a decrypter configured to decrypt encrypted content when activated.

Rabowsky teaches a decrypter configured to decrypt encrypted content when activated (col. 9, line 65 through col. 10, line 11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a decrypter configured to decrypt encrypted content when activated, as taught by Rabowsky, with the system of Angelo et al. It would have been obvious for such modifications because activating the decrypter when only a valid signature was found prevents the playing of data on a tampered system.

Regarding claim 26, the combination of Angelo et al. in view of Rabowsky teaches wherein the boot signature checker is directly coupled to the bus (see fig. 3 of Angelo et al., connection of 208 the to arrows).

Regarding claim 27, the combination of Angelo et al. in view of Rabowsky teaches wherein the boot signature checker is coupled to the decrypter so as to provide the boot signature to the decrypter (see fig. 2, ref. num 72 connected to 74 of Raboswky).

Regarding claim 28, the combination of Angelo et al. in view of Rabowsky teaches wherein the boot signature checker and the decrypter are integrated within a single physical device (see fig. 2, ref. num 72 and 74 within 60 of Rabowsky).

Regarding claim 29, Angelo et al. teaches a computer system capable of decrypting encrypted content, wherein the computer system comprises:

- A processing device (fig. 3, ref. num 200);
- A memory device (fig. 3, ref. num 202 and 204);

- A bus coupled to the processing device and the memory device (fig. 3, the connections between processor and the two memories) and;
- A means for calculating a boot signature, separate from the processing device, that is a function of the signal sequence experienced on the computer system bus **between the processing device and the memory device** during booting up of the computer system (fig. 3, ref. num 208 and fig. 4A, ref. num 308 and col. 1, lines 32-42 and col. 6, lines 20-30).

Angelo et al. does not teach a decrypter configured to decrypt encrypted content when activated.

Rabowsky teaches a decrypter configured to decrypt encrypted content when activated (col. 9, line 65 through col. 10, line 11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a decrypter configured to decrypt encrypted content when activated, as taught by Rabowsky, with the system of Angelo et al. It would have been obvious for such modifications because activating the decrypter when only a valid signature was found prevents the playing of data on a tampered system.

Regarding claim 30, the combination of Angelo et al. in view of Rabowsky teaches wherein the means for calculating a boot signature comprises the following:

- **A processing device**; a **memory device**; a **bus coupled to the processing device and to the memory device of the means for calculating a boot signature** (see fig. 3, ref. num 208 of Angelo et al., the boot block performs steps/instructions and would therefore need processing capabilities along with memory for storing the steps/instructions to be performed); **and**
- A boot signature checker that is coupled to the **computer system** bus so as to be able to monitor the bus for signal sequences (see fig. 3, ref. num 208 of Angelo et al.).

Regarding claim 31, the combination of Angelo et al. in view of Rabowsky teaches further comprising the following:

- A decrypter (see fig. 2, ref. num 74 of Rabowsky); and
- A dedicated connection connecting the boot signature checker with the decrypter (see fig. 2, connection between 72 and 74 of Rabowsky).

Regarding claim 32, the combination of Angelo et al. in view of Rabowsky teaches wherein the boot signature checker, the dedicated connection, and the decrypter are integrated within a single physical device (see fig. 2, ref. num 72 and 74 within 60 of Rabowsky).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Hoff

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100